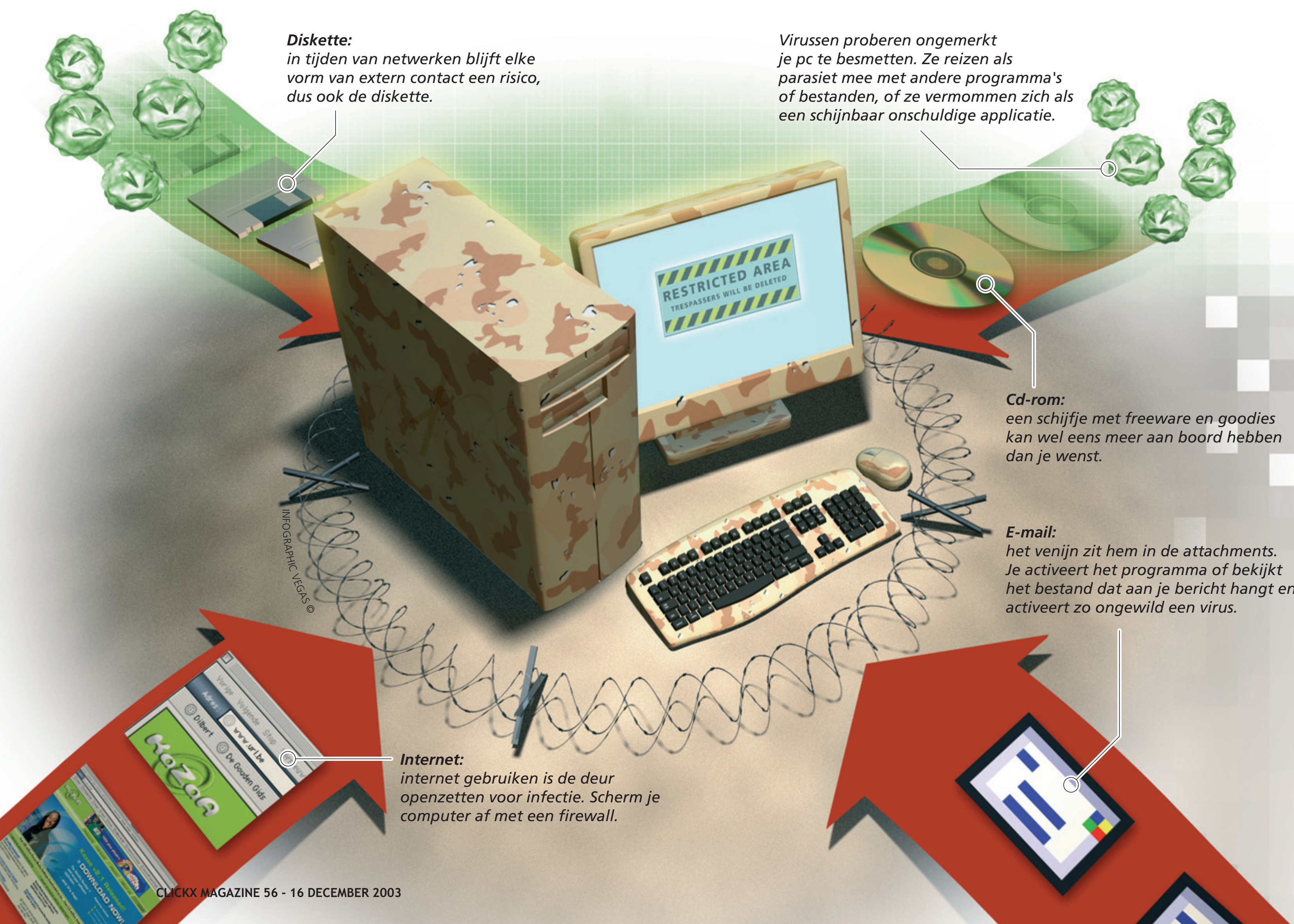
Een computervirus

Elektronische infectie

Virussen zijn niet alleen gevaarlijk voor mensen, ook computers kunnen er flink last van hebben. We hebben het dan natuurlijk niet over een biologisch, maar wel over een computervirus. Ongelooflijk hoe een klein maar vernuftig stukje software verantwoordelijk kan zijn voor zoveel ellende. Clickx steekt zijn nieuwsgierige neus in onkoosjere zaken en beschrijft hoe een virus eruit ziet.

Computervirussen bestaan al langer dan vandaag, maar het is pas sinds kort dat ze veel media-aandacht krijgen. Sommige virusvarianten halen zelfs het zevenuurjournaal. De reden voor de toegenomen aandacht hoef je niet ver te zoeken: een virus kan een grote invloed hebben op de leef- en werkwereld van iedereen! Dat komt omdat computers, veel meer dan vroeger, met elkaar verbonden zijn – via een netwerk of het internet – en bijgevolg gemakkelijker en sneller geïnfecteerd kunnen geraken. Een goed uitgekiend virus verspreidt zich razendsnel en kan verantwoordelijk zijn voor heel wat kopzorgen en zelfs economische schade. Bij je thuis kan het Windows helemaal in de soep laten draaien of bestanden onleesbaar maken of zelfs wissen. En ook bedrijven ontsnappen niet aan de bedreiging van virussen. Vooral hun e-mailservers krijgen het tegenwoordig hard te verduren. Wanneer zo'n belangrijke communicatiemachine vertraagt of zelfs tijdelijk niet meer kan werken, heeft dat ook zijn gevolgen voor heel wat bedrijfsactiviteiten.



Maar ook als je helemaal niets met computers te maken hebt, kan een virus voor problemen zorgen: denk maar aan belangrijke computersystemen zoals die van banken, vliegha-vens of beurzen.

Waar komen jullie toch vandaan?

Wat is een virus? Simpel gezegd is het software die als bedoeling heeft zich te verspreiden en daarbij op een of andere manier schade aan te richten. Best grappig is dat Windows volgens sommigen perfect beantwoordt aan deze omschrijving...

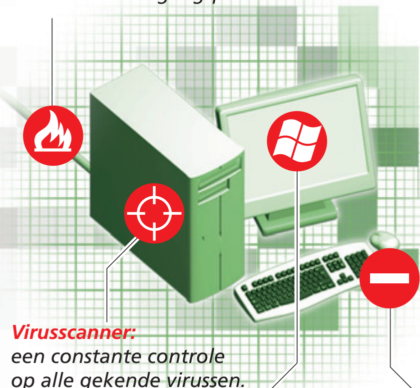
Er zijn verschillende manieren waarop een virus zich kan vermenigvuldigen, maar er is wel altijd 'iets' nodig om het proces in gang te zetten. Dat kan eenvoudig het dubbelklikken zijn op een besmet bestand, maar ook door het openen van een e-mailbericht of zelfs tijdens het surfen komen virussen je computer binnen. Veel virussen maken daarbij gebruik van een of ander veiligheidslek in je software, terwijl andere dan weer rekenen op de nieuwsgierigheid van gebruikers. Eén ding is alvast duidelijk: de tijd dat virussen enkel via diskettes of cd-roms op pc's terechtkwamen, ligt al lang achter ons.

Natuurlijk ontstaan virussen niet uit zichzelf. Virussen bestaan uit programmacode, en daar is programmeerwerk voor nodig. Iemand moet dus een programma ontwerpen en schrijven in een bepaalde programmeertaal. Virusmakers hoeven daarbij niet telkens opnieuw het warm water uit te vinden: de broncode van heel wat virussen is vrij beschikbaar op het internet. Succesvolle virussen krijgen dan ook snel navolging van aangepaste versies of varianten.

Wie zijn de mensen die virussen schrijven, en vooral, waarom doen ze het? Naar de antwoorden daarop kunnen we alleen maar gissen. De ene virusmaker ziet het waarschijnlijk als een uitdaging, de andere doet het voor het plezier of om de aandacht. Als we de berichtgeving mogen geloven, houden zelfs terroristische organisaties zich bezig met het maken en uitsturen van virussen! Virusbouwers mogen echter in geen geval denken dat ze onopspoorbaar zijn.

Een virus kan van je pc een waar slagveld maken. Ook hier geldt: vermijden is beter dan genezen.

Firewall: ben je verbonden met een netwerk, dus ook internet, dan beveiligt een firewall alle toegangspoorten.



Virusscanner: een constante controle op alle gekende virussen.

Updates: virussen gebruiken de zwakke punten van je software. Gebruik steeds de meest recente versie van je besturingssysteem.

Gezond verstand: bedwing je nieuwsgierigheid en open geen vreemde of verdachte files.

Soorten virussen

De mogelijkheden voor virussen om zich te verspreiden zijn erg talrijk, zoveel is zeker. Het mag dan ook niet verbazen dat niet alle virussen op hun rooftocht op dezelfde manier tewerk gaan. Het ene virus komt binnen via e-mail, terwijl het andere zich vasthecht aan een op het eerste gezicht onschuldig programma. En dan zwijgen we nog over de vele mogelijke gevolgen van een infectie: gewiste bestanden, Internet Explorer die rare dingen doet, je besturingssysteem dat de geest geeft, enzovoort. Afhankelijk van de verspreidingsmanier kunnen we virussen onderverdelen in verschillende families. Een overzicht van de meest verspreide virusvormen:

Het **klassieke virus** verspreidt zich door zich te hechten aan een applicatie. Iedere keer als jij die applicatie opstart, treedt het virus in werking, meestal zonder dat je hier iets van merkt. De applicatie is in dat geval geïnfecteerd en het virus kopieert zich naar andere programma's. De enige vereiste is uitvoerbare programmacode. Dergelijke code is gemakkelijk herkenbaar: alle bestanden met de extensie .exe kan je aanklikken en uitvoeren en vormen dus een mogelijk gevaar. Varianten op dergelijke virussen zijn **bootsectorvirussen**. Zij nestelen zich in het opstartsysteem van de harde schijf en kopiëren zichzelf bijvoorbeeld naar diskettes. Gelukkig vormen al deze virussen geen al te groot gevaar meer: ze zijn bekend bij alle virusscanners en moesten ze toch in werking treden, dan worden ze meteen geblokkeerd.

Sommige virussen gedragen zich als het bekende **paard van Troje**. Onder het mom van een of ander onschuldig ogend programmaatje komen ze op je pc terecht. Het programma in spe doet schijnbaar goed zijn werk – bijvoorbeeld een simpel spelletje – maar lanceert tegelijkertijd een aanval op je pc. Het (gedeeltelijk) wissen van de harde schijf blijkt een veel voorkomend gevolg van Trojaanse paarden. Alvast één positieve noot is dat Trojaanse paarden geen mechanisme bevatten om zichzelf te verspreiden. Ze zijn met andere woorden compleet afhankelijk van het feit of je het programma al dan niet installeert.

De meest beruchte vorm van virusverspreiding is die via **e-mail.** Een goed voorbeeld van een e-mailvirus is het Melissa-virus, dat in 1999 furore maakte en opviel door zijn supersnelle verspreiding. Dergelijke virussen komen je pc binnen via een e-mailbericht en maken daarna gebruik van het adresboek om zichzelf (ongemerkt) door te sturen naar al je contactpersonen. Het venijn van een e-mailvirus zit hem meestal in het *attachment* en niet in het e-mailbericht zelf. Attachments zijn bestanden die je koppelt aan een e-mail en die meegestuurd worden. Het kan daarbij gaan om foto's of mp3'tjes, maar ook een PowerPoint-presentatie of een programma kan zo uitgewisseld worden. Handig, dat wel, maar slimme virusbouwers maken hiervan listig gebruik om virussen te laten ontplooien. Zodra je dubbelklikt op het attachment, wordt het virus geactiveerd. Dat kan in principe enkel met uitvoerbare programmacode (zoals een .exe-bestand), maar dat is buiten de vindingrijkheid van de virusmakers gerekend. Attachments krijgen soms erg lange namen, waarbij het onduidelijk is om wat voor soort bestand het gaat. Het wordt zelfs nog gevaarlijker als je weet dat ook een onschuldige PowerPoint-presentatie of een Word-document een virus kan bevatten en in gang zetten. Door de toenemende dreiging van e-mailwormen timmerde Microsoft Outlook (Express) zowat helemaal dicht en weigert het programma nu de meeste soorten attachments te aanvaarden.

Hoe werkt?

Ook de internetproviders wapenen zich meer en meer tegen dergelijke virussen. Ze voorzien hun e-mailservers van automatische scans en leggen beperkingen op inzake toegelaten attachments.
Je hebt ze vast al eens in je mailbox gevonden: e-mails waarin wordt gewaarschuwd voor een of ander nieuw maar bovenal gevaarlijk virus. En wat blijkt na controle? Inderdaad, het genoemde bestand staat wel degelijk op de harde schijf van jouw pc. Er moet dus wel een virus rondwaren, niet? Toch niet, want meestal gaat het om een valse bewering of **hoax**. Een goed voorbeeld van zo'n *hoax* is de e-mail waarin beweerd dat het bestand Sulfnbk.exe een virus is. Dat bestand blijkt op zowat iedere Windows-pc terug te vinden... maar Sulfnbk.exe heeft totaal niets met virussen te maken. Het maakt zelfs deel uit van het Windows-besturingssysteem! Verwijderen is dus helemaal niet nodig. Een lange lijst met hoaxes vonden we terug op de website van Symantec [**www.symantec.com/avcenter/-hoax.html**].

Remedies

Virussen vormen een niet te onderschatten dreiging voor iedere computergebruiker. Zeker als je pc met het internet verbonden is en je regelmatig e-mailt, vergroot de kans dat je zo'n beestje binnenkrijgt. De eerste remedie tegen virussen zijn vanzelfsprekend virusscanners. Deze programma's hebben als doel het opsporen van virussen (zowel in bestanden als in e-mails) en ze te verwijderen. De nieuwste generatie virusscanners biedt daarbij een constante controle op de achtergrond en kan zich zelfs wapenen tegen onbekende virussen. Algemeen verspreide virusscanners zijn die van McAfee en Symantec, maar er bestaan er natuurlijk nog veel meer. In Clickx nummer 52 vind je een uitgebreide vergelijkingstest van virusscanners.
Naast een virusscanner vinden we een firewallprogramma een onmisbaar hulpje. Firewalls detecteren geen virussen, maar door hun manier van werken zijn ze wel in staat om bepaalde virusvarianten te blokkeren. Een firewall controleert alle netwerktoegangspoorten van je pc en sluit ze af. Een goede en gratis firewall is ZoneAlarm van ZoneLabs [**www.zonelabs.com**].
Naast de juiste opspoorsoftware is het minstens even belangrijk om alle kritieke updates voor Microsoft-programma's te installeren. Je mag immers niet vergeten dat veel virussen de veiligheidslekken van software uitbuiten. Het is dus zaak die lekken zo snel mogelijk te dichten en altijd up-to-date te zijn. Voor alle versies van Windows doe je dat het snelst door de Windows Update-site [**windowsupdate.microsoft.com**] te bezoeken. Daar wordt je pc geanalyseerd en krijg je een overzicht van de te installeren pakketten. Dit werkje doe je best wekelijks of laat je volautomatisch uitvoeren door Windows XP of 2000. Ook voor MS Office bestaat een dergelijk updatesysteem.
En last but not least: vergeet het gezond verstand niet! Verwijder verdachte e-mails resoluut en download geen bestanden waarvan de herkomst onduidelijk is. Een gewaarschuwd surfer is er twee waard...

— Bart Stoffels —

VAKTAAL

Attachment: Ook bijlage genoemd. Een e-mailbericht bestaat standaard alleen uit tekst, maar je kan er ook een attachment aan koppelen. Zo'n attachment kan een Word-document of een afbeelding zijn die dan als het ware in een aparte enveloppe bij het e-mailbericht wordt gevoegd. De ontvanger kan die bijlage apart openen en bewaren.

Hoax: Nepvirus. Een hoax is een waarschuwing in de vorm van een e-mailbericht voor nieuwe (al dan niet echte) virussen die erg veel schade kunnen aanrichten. Ze zijn bedoeld om zoveel mogelijk mensen de stuipen op het lijf te jagen. Wie zo'n bericht ontvangt, wordt aangespoord om het door te sturen naar al zijn kennissen om hen ook te waarschuwen. Op die manier willen de bedenkers een massale e-mailstroom genereren in de hoop zo hetzelfde effect te bereiken als een wormvirus: het e-mailverkeer vertragen en e-mailservers lam leggen.